Cross Device Flows

Pieter Kasselman    Daniel Fett    Filip Skokan

IETF 115 London (Nov 2022)
Date: 9 Nov 2022
MIND THE GAP
Today’s Discussion

The problem
The journey (thus far)
Risk Mitigation Framework
What’s in the Draft Proposal
Where we go next
Anatomy of an attack

- Social Engineering
  - Open attachment
  - Click a URL
- Browse to a website
- Brute force account or use stolen account credentials
- Exploitation & Installation
- Command & Control
- Attacker collects reconnaissance & configuration data
- Attacker exploits protocol technical design or implementation issues
- User account is compromised
- Attacker attempts lateral movement
- Privileged account compromised
- Domain compromised
- Exfiltrate data
- Attacker accesses sensitive data
Where Protocol Analysts and Standards Experts Focus

1. Social Engineering: Click a URL
2. Open attachment
3. Browse to a website

- Brute force account or use stolen account credentials
- User account is compromised
- Attacker attempts lateral movement
- Privileged account compromised
- Domain compromised

- Attacker exploits protocol technical design or implementation issues
- Attacker collects reconnaissance & configuration data
- Attacker accesses sensitive data
- Exfiltrate data
Mind the Gap – Where Attackers (often) Enter

Social Engineering
- Click a URL
- Open attachment
- Browse to a website

Exploitation & Installation
- Brute force account or use stolen account credentials
- User account is compromised
- Domain compromised

Command & Control
- Attacker exploits protocol technical design or implementation issues
- Attacker attempts lateral movement

Attacker collects reconnaissance & configuration data

Privileged account compromised

Exfiltrate data

Attacker accesses sensitive data
Social Engineering Exploit (1 of 5)

1. Get a Code

Attacker Controlled Device (Initiate Session)

Authorization Server

Endpoint

Authorization Device (Authenticate/Authorize)
Social Engineering Exploit (2 of 5)

1. Get a Code
   Attacker Controlled Device (Initiate Session)

2. Change Context
   Click here to sync your messages

Authorization Server
Endpoint

Authorization Device (Authenticate/Authorize)
Social Engineering Exploit (3 of 5)

1. Get a Code
2. Change Context
   Click [here](#) to sync your messages
3. Scan or enter a Code, click on link Authorization Device (Authenticate/Authorize)
Social Engineering Exploit (4 of 5)

1. Get a Code

2. Change Context

3. Scan or enter a Code, click on link

4. Authenticate/Authorize

Click here to sync your messages

Authorization Server

Endpoint

Attacker Controlled Device (Initiate Session)

Authorization Device (Authenticate/Authorize)
Social Engineering Exploit (5 of 5)

1. Get a Code
2. Change Context
3. Scan or enter a Code, click on link
4. Authenticate/Authorize
5. Retrieve Tokens

Click [here](#) to sync your messages

Authorization Device (Authenticate/Authorize)
Social Engineering Exploit

1. Get a Code
2. Change Context
3. Scan or enter a Code, click on link
4. Authenticate/Authorize
5. Retrieve Tokens

Authorization Server
Endpoint

1234

Click here to sync your messages

Attack Pattern Summary: Exploit the Unauthenticated Channel
1. Initiate the session, retrieve code (QR code, user code)
2. Use social engineering to change context and persuade user to authorize session (illicit consent grant)
3. Bypasses multi-factor authentication (don’t need to harvest credentials)
Homo Securitus to the Rescue

Homo Securitus
1. A security expert
2. Knows how the protocol should work
3. Detects a social engineering attempt
4. Is laser focused on current context
5. Foolproof mitigation for cross device flows

But is a rare species....
But what about Homo Sapiens?

Homo Sapiens
1. “Expertise elsewhere” - not a security expert
2. Busy and in a rush, needs to get things done
3. Worries about breaking things
4. Wants to help

Needs to make fewer decisions,
Needs help to make better decisions
Needs protection even if a bad decision is made
Points to ponder...

Attacks exploit the unauthenticated channel between initiating and authorising device

Homo Securitus vs Homo Sapiens
• Pushing responsibility on Homo Sapiens to “authenticate” the channel...

Cross Device Flows spans multiple protocols and scenarios
• Device Authorization Grant
• But also:
  • Client Initiated Backchannel Authentication (CIBA)
  • Wallet invocation (OIDF SIOP, OIDC for VCs)
  • Session transfers/Application Bootstrapping
  • Authentication (W3C WebAuthn/FIDO)
The Journey (thus far)

OSW 2022/Identiverse
Call for solutions

IETF 113
 Solicit interest

IETF 114
 Update on progress/findings

Attacks

OSW 2021
1st Description
Mitigation Framework – Closing the Gap

Pragmatic Mitigations

- Authenticated Channel
  - Authorization Code Grant
  - Client Initiated Back Channel Authentication
  - Device Authorization Grant

- Unauthenticated Channel

Explore Alternatives

Foundational Underpinnings

- Authorization Server
- Endpoint

Sequence:
1. Wake up authorization device in the wallet
2. Refine the action request using the wallet's service
3. Paired items with service and authorization device application
Draft Proposal for Cross-Device BCP

Uploaded to Datatracker: draft-kasselman-cross-device-security-00 - Cross Device Flows: Security Best Current Practice (ietf.org)
2. Cross Device Flow Concepts

2.1. Example A1: Authorize access to a video streaming service

2.2. Example A2: Authorize access to productivity services

2.3. Example A3: Authorize use of a bike sharing scheme

2.4. Example A4: Authorize a financial transaction

2.5. Example A5: Add a device to a network

2.6. Example A6: Remote onboarding

2 Additional use cases suggested since publishing draft
What’s in the Draft Proposal: Attacks

3. Cross-Device Flow Exploits
   3.1. Example B1: Illicit access to a video streaming service
   3.2. Example B2: Illicit access to productivity services
   3.3. Example B3: Illicit access to physical assets
   3.4. Example B4: Illicit Transaction Authorization
   3.5. Example B5: Illicit Network Join
   3.6. Example B6: Illicit Onboarding
   3.7. Out of Scope

1 Additional attack suggested since publishing draft
What’s in the Draft Proposal: Mitigations

2 More community contributed mitigations since publishing draft

<table>
<thead>
<tr>
<th>Mitigation</th>
<th>Prevent</th>
<th>Disrupt</th>
<th>Recover</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish Proximity</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Short Lived/Timebound Codes</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Content Filtering</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Trusted Devices</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Trusted Networks</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Limited Scopes</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Short Lived Tokens</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Rate Limits</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Sender Constrained Tokens</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>User Experience</td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

Table 1: Practical Mitigation Summary
# What’s in the Draft Proposal: Protocol Selection Guidance

<table>
<thead>
<tr>
<th>Description</th>
<th>Susceptibility</th>
<th>Mitigations</th>
<th>Device Capabilities</th>
<th>When to Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Authorization Grant</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client Initiated Backchannel Authentication</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FIDO2/WebAuthn</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5.2. Protocol selection ........................................18
5.2.1. IETF OAuth 2.0 Device Authorization Grant RFC8682: ........................................18
5.2.2. OpenID Foundation Client Initiated Back-Channel Authentication (CIBA): ..................19
5.2.3. FIDO2/WebAuthn ........................................20
What’s in the Draft Proposal: Foundational Pillars

Formal analysis against OAuth Protocols have been effective
Limited formal analysis of cross-device flows
• Humans are modelled as error free decision makers
• Modelling flawed decision-making may help evaluate effectiveness of mitigations

To ensure secure cross-device interactions, a formal analysis using the WIM therefore seems to be in order. Such an analysis should comprise a generic model for cross-device flows, potentially including different kinds of interactions. The aim of the analysis would be to evaluate the effectiveness of selected mitigation strategies. To the best of our knowledge, this would be the first study of this kind.

Modeling Human Errors in Security Protocols

David Basin  Saša Radomirović  Lara Schmid
Institute of Information Security, Department of Computer Science, ETH Zürich
Email: {david.basin, sasa.radomirovic, schmidla}@inf.ethz.ch
What Next?

OSW 2022/Identiverse
Call for solutions

IETF 113
Solicit interest

Attacks

OSW 2021
1st Description

IETF 114
Update on progress/findings

IETF 115
BCP Draft